# INTRODUCTION

In the not so distant past, countersigns (what we would identify now as passwords) were reserved for the military and secret society [1]. They were used usually only in two circumstances: to identify messages from potentially unknown correspondents and to identify persons when other, more direct means were inadequate or unavailable [1]. This system obviously had its flaws, but given its rather limited use, its served its purpose more than adequately. In fact, one could argue that its main advantage was is ease of use; it’s very simple to remember one or two short phrases and repeat them back on demand. Of course, to be clear, it was only the *second easiest* to use method of identifying people. The *easiest* to use method, of course, belongs to the so-obvious-it-is-overlooked ability of human beings to identify one another by sight and, to a lesser degree, by sound. Pass phrases were only used (despite the lessened security and ease of use) because they could be used when visual identification was difficult or impossible, such as at night, when writing a letter, or when speaking over a phone [1]. Fast forward a few decades, and the designers of the first computer system were in need of a simple way to secure their new projects against random passersby [2]. With these researchers needing a quick way to secure their system, combined with the fact (which alone would have likely been enough to send user authentication down this route) that these systems could only accept text based input, the choice was obvious: simply have the user enter a string only they know, problem solved [2]. Of course, they could have used other things rather than random strings of characters, such as knowledge based tests, but no one wanted to devote the resources to such an ancillary task [2]. And to be fair, at the time, this system was **more** than secure enough for their purposes [2]. When the worst attack that one is defending against is a nosy colleague attempting to look at/mess with your system, the randomness of even a 3-character passcode would be enough [2]. The problem, as it so often is in the field of computer science, is that this early use case quickly grew so very far beyond what these early designers envisioned even in their wildest fantasies [3]. And with this growth, passwords were carried along for the ride. And so what was once a good, reasonable, and very practical choice, becomes the bane of every security researcher in the modern world. Of course, we have to be careful not to condemn those whose have brought us to this point, for three very simple reasons. First, while computers did indeed grow very quickly, there were no sharp jumps; there never was a time in which it suddenly became clear that computers had evolved completely from their original use cases, and that it was time to start removing/changing some of the early “just enough to get by” features [3]. By the time any of this every became clear, it was too late, passwords (and many other features) had become too ingrained – and outside the control of those who knew to change them – for them to be switched out for an alternative 3[]. In fact, passwords were, up until the widespread advent of the internet (and even somewhat after) a sufficient security measure, provided they were long enough, not-shared, etc., which was much easier to accomplish back then [3]. Secondly, even if there had been an obvious liminal period where it was time to start polishing up some of the feature because computers were about to go mainstream, there was – and as we will discuss **still isn’t** – a clear alternative to passwords [4]. Nothing matches their ease of use, portability, and simplicity in all, or even most, dimensions [4]. And while almost all other proposed solutions offer better security, unless forced by some authority, users are extremely unlikely to switch over unless the new solution is at least as good as passwords on the three previously mentioned things [4]. And the last point that is quickly revealed in reading the literature, is that it is not that passwords are fundamentally flawed, it is that the system in which we’re using passwords (i.e. multiple websites logins, computer logins, phone passwords, pin codes, etc.), the necessary security, and passwords are fundamentally opposed [4]. You can have any two, but not all three. This is basically due to the limits of human beings: we only have so much capacity to remember passwords, with the number of passwords we can remember going down as the security (and therefore complexity) of them going up [5]. This was fine a hundred years ago when only two or three simple, very memorable pass phrases were needed. This was fine when only two or three simple passwords were needed for the first computer systems. This was fine even for the first few years of the internet, when security was not important, attacks were far less prevalent, and most importantly, their simply were not that many passwords that needed to be remembered. Now, however, the average user has over **90** online accounts, each with its own password to remember. Having nice, complex passwords for all of these sights is simply a task that is too complex for a human being to manage [5]. Again, this was something that no one saw coming; it arose dynamically out of the huge explosion of the web in the 90s, and by the time everyone noticed how annoying, and (because users hate annoying), how insecure everything was getting, it was too late to institute any major changes. Of course, this problem has been one of the most studied problems in computer security, and many solutions have been proposed. Some merely augment passwords, some changes the infrastructure significantly, and many do away with passwords altogether. Of these, only those of the first kind, and only two of those, have seen some kind of mainstream adoption: password managers and two-factor authentication. The first we will discuss later, since its use is relatively low among the mainstream users. The second, however, has become increasingly popular over the last several years as a way to shore up the security for critical sights (such as banking, other financial institutions, and sites that have the ability to do significant damage to personal character) [6]. Specifically, it shores up the weakness that even if a password is compromised, without the physical two-factor authenticator, the account is still safe [6]. This is far from ideal, but much better than the plain setup of just a password [6].

# Passwords and why they suck

As we’ve previously hinted at, passwords themselves are relatively secure. When we talk about good passwords, we’re usually referring to the level of entropy (or, in simple terms, its difficulty to guess in a timely manner given current technology) a password has [7]. Using this, 123456abcdef is horrible, while a perfectly random set of 12 characters is sufficient [7]. Bumping it up to ten makes it near impossible to crack. Going back to the perfectly random 12-character password, that would take around a millennium to crack with sustained effort by hardware capable of 1,000,000,000,000 guesses per second is on the order of 20 days (assuming 75-character option chosen from). And the hardware to guess 1,000,000,000,000 passwords/s is something that is only brought to bear against extremely valuable targets. The problem lies in the fact that humans do not choose perfectly random passwords [8]. People choose names and dates that are significant to them, they almost always base their password off a dictionary word, the choose easily guessable runs of numbers, the special characters they use are heavily weighted towards a few common ones, the list goes on [8]. All of these things add up to make passwords far less secure than their theoretical performance [8]. It brings down the difficulty for a millennium for a single password to a few hours for several thousand passwords [9]. And that was not an experimental list of passwords; those were real passwords that were leaked that were ran on a real production system [9]. People absolutely love to use passwords like 12345, or abcde, or [first name] + [last name] + 1 [9]. Worse still is that people constantly reuse their password across multiple sites, increasing the chance that if one password is compromised, then all of their passwords are compromised [5]. Of course, as was mentioned above, people constantly reusing passwords is not a deliberate attempt on their part to thwart security researchers, or even a manifestation of their laziness: it is simply a survival tactic [5]. When people are asked to make passwords that must “be at least 8 characters are longer, contain a latter, a number, and a special character” for **90+** sites, something has to give. So users will either make the passwords technically follow the rules, but in a very easily guessed manner (such as [first name] + [number(s)] + [!]) and give that to the site [9]. Or they’ll make a complex password but reuse it among many (or all sites) [5]. In fact, as evidence that users are at least somewhat aware of and caring about security, many users will have a few passwords, with one being for “don’t care” sites, as in sites that a breach would matter little, such as a Netflix login, a password for more important sites, like Facebook, and finally a password for financial institutions that has the highest strength [16]. This shows that users care about having security on their sites, but are incapable (by human nature) of memorizing all the long strings that would be required to make it necessary [6]. To this ends, some people will, either as an augment their ability to memorize “good” passwords, or as a consequence of too onerous a demand by whatever company, organization, or site they are setting up an account with, write their passwords down. Now, anyone with a background in security research will likely be shaking their head at the utter stupidity of users demonstrated by defeating the entire point of passwords by leaving them **in plain sight where anyone can see**. But we must keep two points in mind. The first is that, as was mentioned above, some sites people simply care less about if they are breached (so long as they are recoverable eventually) [16]. They have good reason to do so, because some sites simply are less damaging if they are compromised, and less disruptive when they are. So as long as passwords keep the breach rates acceptably low, then the user is happy and everyone is fine. The second fact is that passwords in today’s world are much more concerned with keeping out actors with whom one’s only interaction with is over the internet, and less with those one interacts with on a day to day basis. With this thought in mind, it could very well be an acceptable risk to keep most passwords written down, and keep only the high valuable ones memorized [16]. Of course, this does increase the risk of a *local* malicious or opportunistic attacker who had access to wherever the passwords were written down, such as janitorial staff seeing a sticky note on a compute in an office, gaining access, but in many cases that risk is acceptable [16]. And should the medium on which the passwords are written be carried with one’s person, then all the better. This very scenario has actually been advised by very high profile security researchers to help alleviate the problem described above of too many passwords, and allow users to keep those accounts that have the capacity of being truly damaging (such as highly connected social media accounts as well as financial institutions) [16]. Of course, and to be clear, this is more of a stopgap measure than anything else. The problems that we’ve been discussing have only come about in modern days for two reasons: lots of accounts that need separate passwords and the needed passwords getting more and more complex [16]. The first problem is one that we’ve mentioned again and again, but we’ve never described why exactly the current most popular (if insecure) solution of reusing passwords on multiple sites is insecure. In a perfect world, it would not be. If every website visited used current state of the art encryption algorithms, insured all their equipment was correctly configured and updated, and followed current best practices in security, then reusing passwords would be very acceptable. In fact, using the same password even after one of the sites its used on is breached would be acceptable, since, by current standards, no plaintext, or even encrypted passwords should ever be stored, only their hashes. But, as in clear, we do not live in a perfect world and most (all) websites do not come anywhere close to storing passwords according to best security practices. So utilizing a password on more than one means that, basically, the security of your password, and therefore all your sites, is the same as the security of the weakest site you used the password on [16]. And that is often very weak indeed. But another problem is there is no way to know which sites have good security, and which have bad. So every time you reuse a password, it’s a bit like playing Russian roulette. This is further compounded by the second problem that the ability of attackers to crack passwords grows every year right along with the advances in computing power (thank you Alan Moore), but human minds stay static. Humans have only a limited capacity to memorize passwords, and the more complex they get, the fewer we can handle [16]. But in our current situation, passwords are getting both more numerous **and** more complex. And that is why passwords must be dethroned, if not now, then sometime soon. And this has just been discussing the vulnerabilities inherent in passwords themselves. So far, we have overlooked things like the ability to reset passwords by knowing the answer to a few “secret” questions such as mother’s maiden name (which the rise of social media has made almost trivial to find) or the attacks that passwords are inherently weak too, such as replay attacks, man-in-the-middle attacks, etc. Since something needs be done about the weaknesses of passwords as they are currently used, plus the weakness just mentioned, most sights have begun rolling out something called two-factor authentication. This appears to be the future of sites which are considered to need high security, at least for the short-term.

# Two-factor Authentication and why it’ll save your life

To understand what two-factor authentication (TFA) is, we must first understand the three generally recognized types of factors (methods or things) that can be used to (uniquely) authenticate (or verify the identity of) you [12]. These types are what you are (biometrics) what you have (a cellphone, token authenticator, etc.), and what you know (passwords) [12]. TFA refers to using at least one factor from exactly two of these types [12]. In most usages encountered today, these are passwords plus something you have, like a phone or a device to generate tokens, but in principle they could be iris recognition plus the smartwatch on your wrist [12]. The important thing about TFA is that it leverages the strength of both of its methods to shore up each other’s weaknesses [12]. For example, passwords are rather easy to steal, especially without the knowledge of the owner (who could otherwise take steps to prevent any damage occurring from the loss, such as changing the password), but mobile phone TFA (MPTFA) – which is the main TFA used by most users, or very similar to the TFA used by most users and is therefore what we will focus most of our attention on) is not [12]. A hacker in India can easily steal the password of someone in America, but acquiring their mobile phone is something that would be much, much more difficult. Better yet, even if some malicious hacker did somehow acquire both the mobile phone and password, the user would near immediately be aware of the loss of the former, and could take steps to secure the now vulnerable accounts (this would occur whether the user was doing it specifically to make sure that their user accounts could not be breached or if they were doing it to simply set up a new mobile device). This also protects users from things like phishing (since a TFA cannot be copied and whatever signal is sent usually is only valid for a short period of time) as well as man-in-the-middle attacks [12]. Basically, TFA that is perfectly implemented counters all the vulnerabilities of passwords except for the much rarer cases of when the attackers are agents who are nearby or somehow have the resources to acquire the mobile phone [12]. This means that the vast majority of users would be protected. Obviously, no TFA implementation is perfect, and even disregarding that, TFAs have inherent downsides. They are much more easily lost than passwords, unlike passwords (which a user does not actually have to take with them) a user must make sure to carry the mobile phone with them lest they be locked out of their accounts [6]. Then there’s the more worrying problem: what happens if/when something happens to the mobile phone? While it’s random or unpredictable, almost every has broken or lost their phone or is close to someone who has [6]. By its very nature, the MPTFA cannot be something that can be easily ported to anther phone without the working original at the very least. And since people would be completely unwilling to use a service that made it possible that they could completely lose access to their accounts, there must be some method to recover access should the mobile phone be damaged or lost [4]. But this introduces a dangerous flaw that can undermine the entire point of TFA; should the only check to remove TFA be to send a verification email (which many sites use), or to answer a few security questions (which even more sites use), TFA is useless [6]. All an attacker has to do is answer those security questions (a task which is much easier than directly breaking the TFA thanks to the rise of social media as well as the ease at deploying social engineering) to break into the account [6]. This is not even getting into the other vulnerabilities that can undermine TFA, such as incorrect or insecure implementation by the offering website or service or the ability for malware which has infected a PC (and can therefore siphon off all passwords that are entered on it) to infect the mobile phone and either steal the secrets it uses to generate the authentication code or to intercept the text messages that are sent to it that contain the mobile authentication code [6]. This is made practical by the fact that a laptop and the phone of its owner very frequently connect to the same local area network (i.e. the Wi-Fi at their home) [6]. So while TFA can indeed improve user security, it is far from a panacea. In fact, it is more, at least in its current form, like a Band-Aid for the problems with passwords. And to be clear, it is only a Band-Aid for **some** passwords. As we have discussed previously, the main thing that either blocks the adoption of an otherwise great technology, or allows the adoption of an otherwise subpar technology, is ease of use [4]. Something that is very convenient to use will almost certainly be much more adopted than something that is more difficult to use, regardless of the relative performance they have on other metrics. And this is exactly the case with TFA. No matter how it is implemented, it makes the usually simple task of logging into a website or service much more complicated [4]. As in, one can no longer simply enter their password [4]. Now one has to enter their password, grab their phone, unlock it, open an app, and transcribe the code therein onto the computer to log in [4]. A much more difficult process comparatively. As such, it is only being rolled out (and utilized on) those sights which carry a high risk should they be compromised, such as email accounts, bank accounts, and social media accounts. And even then, only a small percentage of users have utilized this feature, though there has been an increasing push to get users on these sites to move to utilizing two factor authentication. Usually this is brought about because it costs businesses, especially banks, money when their customers’ accounts are compromised. This obviously gives them incentive to make user accounts harder to break into. One example is the online gaming service Steam, where users that **do not** have TFA activated face additional restrictions.

# The Future

Of course, as we have mentioned, TFAs in their current form are nothing but a Band-Aid, and one for only a limited number of accounts at that. With the ever increasing number of online accounts a person has, as well as the ever increasing difficulty a password requires to be considered secure, a new solution is not just needed, it is required [4]. The key to that, is ‘in their current form’. While the TFAs are, at current, a stopgap, the technology that underlies them may very well represent the future of passwords [4]. To see why, lets back up a step. The MPTFAs that we discussed so far work as follows, be sign on to an account with their username and password [6]. Assuming that is its correct, they are then asked to enter a code that is generated on their phone [6]. But if your phone is the keys to the kingdom, why not just enter your username into the site and then have your phone, either by communicating to the website through your computer or directly, authenticate you [4]. It itself is already protected by a passcode (or even more convenient, a thumbprint), so it’s a simple matter to authenticate yourself to your phone and let it handle everything else. This immediately solves the problem of having to remember dozens of complex passwords; with your phone handling the authentication, the token that is used to verify that is indeed you trying to access your account can be rendered virtually uncrackable and, better yet, valid only for an extremely short period of time [5]. This protects from a host of vulnerabilities, from replay attacks, to keylogging. Of course, the system is not without its flaws. In fact, this magnifies some of the dangers of MPTFA; at this point, your mobile phone is the lynchpin to your **entire** digital life [4]. Should it ever be lost or stolen, you are in serious trouble. It would take a very significant amount of effort to recover one’s accounts. Worse yet, should one’s phone ever be actually compromised, the attacker now has access to every account you own, making impersonating you all the easier, and reclaiming your accounts all the harder. The solution to this problem then, is to reintroduce TFA. But instead of relying on your mobile phone as the TFA vector, or, indeed, anything that is visible to you, the TFA is your behavior [13]. Specifically, researchers have found, as you might have guessed, that the way we behave is very telling [13]. Take Facebook for example, when logging in, the way a user’s mouse moves across the screen, the speed at which they type their email address, the mistakes they make, their actions they tend to take after logging in, the people and types of post they spend the most time on, etc. are all ways to insure that a person is indeed who they say they are. All of this data can be collected during the first few interactions with the service, and then updated continually thereafter as a person slowly changes. This type of security, when using multiple types of a person’s habits, is nearly impossible to fool without actually having access to the records stored and algorithms used [13]. This is because there are so many variable ways in which a person can perform several actions that the space of all possibilities, even when allowing for the necessary tolerances, is too huge [13]. Of course, this system, like everything ever before it, has its flaws. Chief among them currently is that many if its flaws are unknown, due to the little research and actual testing it has received. But one that is obvious is the difficulty many medium and smaller sized websites would have implementing this system, as well as the resources it would require to constantly monitor and assess hundreds of minute actions by all its users. Luckily, this has been utilized in some form, though not for authentication. Currently, Google and a few other websites utilize mouse movements and other user characteristics to verify that a user is human (and therefore bypass the captcha checks) [14]. Behavioral biometrics represents an extremely rich field for authentication [15]. Amusingly enough, this is analogous to the situation in horror movies when characters claim that another just feels “off”. While it’s hard to name, humans keep tabs on the normal behaviors of those close to use, and if enough of those start being violated, we thing something is wrong. Computers are just now gaining enough power to be able to emulate this.

# Conclusion

It seems clear that, for most applications, the entire idea of remembering strings of characters as means of authentication will soon be dead 4[]. While people have been preaching the death of passwords for over a decade now, they must die soon, or soon the protections on our digital accounts might as well be minor annoyances to those wishes to gain entry [4]. It is both the blessing and the curse of computer science that everything advances at an ever increasing rate. What is state of the art today will be routine in a year and outdated in two. Passwords are a relic from the earliest days of our field, and while they were dragged along this far because of their simplicity, it is time for them to die. Luckily we’re finally hitting the point of being able to implement systems that mimic, in many ways, how humans identify one another [14]. Not only that, we’re finally being able to take advantage of the hyper-connectivity every has, and utilize the devices that are always with them as a proxy to their identity. While change will likely begin to happen ever more quickly now that passwords are hitting a wall, and are being broken more and more easily, it will take time for whatever system we utilize in the future to come about. In the meantime, we can shore up the defenses of our most precious accounts by utilizing TFA, which most often involves our mobile phones in some form. Of course, this is merely prognosticating for the future, and as history has shown us, nowhere is that more dangerous than with technology. We can be sure that the rule of passwords will end soon, but as to what will replace them, well, we may very well find ourselves surprised. After all, it’s always the things that no one suspected that change the world the most.

References

1. “Countersign”. *Merriam-Webster*. Meriam-Webster. Web. 16 April 2016.
2. McMillan, Robert. “The World’s First Computer Password? It Was Useless Too”. *Wired*. Condé Nast, 27 January 2012. Web. 16 April 2016.
3. Hiscott, Rebecca. “The Evolution of the Password — And Why It's Still Far From Safe”. *Mashable*. Mashable Inc., 30 December 2013. Web. 16 April 2016.
4. Bonneau, Joseph, et al. "The quest to replace passwords: A framework for comparative evaluation of web authentication schemes." Security and Privacy (SP), 2012 IEEE Symposium on. IEEE, 2012. Web. 16 April 2016.
5. Czeskis, Alexei, et al. "Strengthening user authentication through opportunistic cryptographic identity assertions." Proceedings of the 2012 ACM conference on Computer and communications security. ACM, 2012. 16 April 2016.
6. Dmitrienko, Alexandra, et al. "On the (in) security of mobile two-factor authentication." Financial Cryptography and Data Security. Springer Berlin Heidelberg, 2014. 365-383. 16 April 2016.
7. Kelley, Patrick Gage, et al. "Guess again (and again and again): Measuring password strength by simulating password-cracking algorithms." Security and Privacy (SP), 2012 IEEE Symposium on. IEEE, 2012. 16 April 2016.
8. “Unmasked: What 10 million passwords reveal about the people who choose them” *WPEngine*. WPEnine, Inc., 2015. Web. 16 April 2016.
9. Goodin, Dan. “Anatomy of a hack: How crackers ransack passwords like ‘qeadzcwrsfxv1331’”. *Ars Technica*.Condé Nast, 27 May 2013.
10. Duffy, Jill. “You Have Exactly Three Passwords, Don’t You?”. *PCMag*. Ziff Davis, 7 June 2011. Web. 16 April 2016.
11. Florêncio, Dinei, Cormac Herley, and Paul C. Van Oorschot. "Password portfolios and the finite-effort user: Sustainably managing large numbers of accounts." 23rd USENIX Security Symposium (USENIX Security 14). 2014. Web. 16 April 2016.
12. Aloul, Fadi, Syed Zahidi, and Wassim El-Hajj. "Two factor authentication using mobile phones." (2009): 641-644. Web. 16 April 2016.
13. Yampolskiy, Roman V., and Venu Govindaraju. "Behavioural biometrics: a survey and classification." International Journal of Biometrics 1.1 (2008): 81-113. Web. 16 April 2016.
14. Greenberg, Andy. “Google Can Now Tell You’re Not a Robot With Just One Click”. *Wired*. Condé Nast, 3 December 2014. Web. 16 April 2016.
15. Gamboa, Hugo, and Ana Fred. "A behavioral biometric system based on human-computer interaction." Defense and Security. International Society for Optics and Photonics, 2004. Web. 16 April 2016.